SOAPware
Application Service Provider Privacy & Security Policies

Access	With the SOAPware Hosting Service, you receive a complete virtual private server allowing you to run SOAPware and a host of other third-party applications from any computer with an Internet connection and a Remote Desktop Protocol application.
Authorization	Authorized users are established by the SOAPware Hosting Service IT dept for the OS, and by the Security Administrator for SOAPware
Authentication	Each Virtual Server has its own NT based security system employing Kerberos authentication methods standard to any Windows 2003 Server OS. The connection using Microsoft's Remote Desktop application uses 128 bit encryption from the server to the client session. User passwords are 13 character pass phrase passwords generated to be easily memorized but extremely hard to socially or brute force hack. Once the session is started SOAPware utilizes its own security methods which are based on internal hashed passwords. The connection from the client is acquired across a firewall allowing only port 3389 to that specific IP. No other ancillary ports are open to the outside network. The connection from the server to the patient data is acquired across another firewall only allowing traffic from that server's IP to the specific port of the database server, thus preventing any internal network peering from one server's database to another.
Audit	7 Day circular logging is kept on the Virtual Servers by default in the Microsoft Event Logs.
Secondary Uses of Data	SOAPware, Inc. will never sell or disclose any personal or clinical information. The data, even though hosted by SOAPware, is fully owned by the users as long as they maintain payment.
Data Ownership	The data generated (Patent Records) is always belongs to the end customer. At anytime the customer can request their databases be sent to them on applicable media, CD, DVD or Hard Drive only incurring the cost of the media and shipping. It is the opinion of the president and founder of SOAPware, Inc. that the customer is always the owner of his data. This data is not utilized (mined) for any third party company without the consent of the owner.